REMARKS

Reconsideration and allowance of the above-referenced application are respectfully requested.

The informalities noted in claims 3, 4 and 10 have been obviated herein by amendment. Applicants apologize for these errors.

A new abstract is presented to obviate the rejections.

Claims 1, 4, 10, 12, 14-16, 18, 20, 21 and 23 stand rejected under 35 USC 103 as allegedly being unpatentable over England at all, referred to herein as 063. This contention is respectfully traversed.

Claim 1 requires encrypting files using an encryption key that is associated with the user, identifying the user, and allowing changes to be made to any of the plurality of files associated with the user, responsive to the identifying. In addition, claim 1 requires reading the files using a recovery decryption key which is intended for recovery of files when the first decryption key becomes unavailable. These features are not taught or suggested by 063.

063 does teach encrypting computer files using an encryption key. However, the rest of the subject matter of claim 1 is not taught, and in fact 063 teaches away from much of the subject matter of claim 1.

Claim 1 requires that when the user is identified, the user can make changes to any of the plurality of files associated with the user. Column 17, which is referred to by the official action as supporting this claimed feature, allows the user to request a key based on their identity. This provides a unique identity for each user. See column 17 lines 42-44. However, in this embodiment, 063 explains that there "must be a way to

recover the keys when the identity changes...". See column 17 line 65-67. Column 18 beginning at line 2 describes storing the keys off-site in a key vault. In other words, 063 teaches an entirely different way of recovering files when the first decryption key becomes unavailable. According to 063, the key is stored off-site, and reconstituted. Claim 1, in contrast, requires using a second, recovery decryption key. 063 teaches away from using this kind of recovery key.

The rejection refers to the ephemeral key disclosed in column 15. The column 15 embodiment is described as being different than the embodiment of column 17. Column 17, line 15, refers to the following section as an "alternative embodiment" see column 17 line 15.

Moreover, even if the subject matter of column 15 and the ephemeral keys are used, it still does not suggest the "allowing reading of said first plurality of files..." limitation of claim 1. Column 15 describes that there are master private keys that are used to certify ephemeral keys, and that these are valid for short period of time. These ephemeral keys are used to sign components, to avoid security issues from the public release of the ephemeral key. However, according to column 15, the ephemeral keys are only used to sign components. Since they are signing components, they cannot be recovery decryption keys, as defined by claim 1.

Claim 1 requires reading the plurality of files, using a recovery decryption key different from the first decryption key. The ephemeral key in column 15 is a signing key, used for signing for a temporary period of time. This certainly does not suggest a recovery decryption key of the type claimed. Signing is not the same as decryption.

Claim 1 should hence be allowable for these reasons.

Claim 10 defines an operating system that operates based on stored files, and detects that an update has been requested for one of the operating system files. The rejection alleges that column 13 lines 3-19 of 063 teaches this. In fact, however, this is incorrect.

Column 13 describes checking the operating system against a log. Column 13 lines 3-18 describes that identities are checked against the list to make sure that nothing has changed. Each of the identities is checked to make sure that the operating system has not been compromised. The second embodiment also uses a boot log, that views OS components that have been loaded, to make sure that the OS components have not been tampered with. There is no teaching or suggestion in this, or any of the other subject matter, of detecting an update that is requested.

According to claim 10, a digital certificate associated with the update is checked over the Internet to see if it matches a prestored criteria. The rejection states that this is taught by 063 column 11 lines 23-51. However, this cited portion describes the boot loader, and teaches nothing about the update, where -- even by the patent office's own interpretation -- the update is not discussed until column 13. The cited section of column 11 only describes testing the identity of the boot block, and testing whether it is proper.

Column 11 lines 32-35 describes that the components may be signed by a trusted source. Column 11 lines 37-38 describes that the signature of the component(s) may be checked before loading it. However, this has nothing to do with an update. Rather, this is simply carried out during the boot process, and teaches nothing about checking a digital certificate for an update prior to allowing the update to

be conducted, as claimed. There is absolutely nothing that could teaches or suggests "allowing the update to be conducted only if the digital certificate matches".

The rejection admits that 063 teaches nothing about carrying this out over the Internet. The rejection alleges that a component revocation list (CRL) may be checked to determine if the component signature has been revoked. The rejection states that this would have to communicate over WAN or Internet. However, this contradicts the specific language of column 12 lines 14-15 of 063 - that the CRL is "provided" -- not available over the Internet. Nothing in columns 6 lines 42-57 or anywhere else in 063 indicates that the CRL would be available over the Internet.

For all of these reasons, it is respectfully suggested that claim 10 is quite different than anything disclosed by 063 and hence wholly unobvious based thereon.

Claim 14 defines that the file accessing part has a recovery key that allows alternatively recovering the files if the first filed decryption key is unavailable. The patentability of this feature has been discussed above. The ephemeral key in 063 does not teach or suggest this feature. Claim 14 should hence be allowable along with the claims that depend therefrom.

Claim 20 should be specifically allowable, since it defines a removable memory and defines that an encrypted file is decrypted prior to writing to the removable memory. Nothing in 063 teaches this. The 'license' simply describes that some things can be encrypted prior to writing. There is no teaching or suggestion, however, of the removable memory, and that an encrypted file is decrypted before being sent to the removable memory.

Claim 23 defines a recovery key, which should be allowable for similar to those reasons discussed above. The ephemeral key in 063 teaches nothing about this recovery key.

Claims 13, 22, 25 and 26 stand rejected over 063 in view of 537 to Tello. This contention is further respectfully traversed. The rejection admits that the "allowing..." part of claim 23 is not taught by 063, but contends that this is shown by '537. This contention is respectfully traversed, however. 537 is cited to show that certain file parts can be stored unencrypted or encrypted. However, claim 22 also requires unencrypted files that can be read and cannot be written to. Nowhere does 063 or 537, or the hypothetical combination thereof, teach or suggest this claimed subject matter.

Claims 8, 9 and others should be allowable by virtue of their dependency as well as on their own merits.

It is believed that all of the pending claims have been addressed in this paper. However, failure to address a specific rejection, issue or comment, does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above are not intended to be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Therefore, and in view of the above amendments and remarks, all of the claim should be in condition for allowance. A formal notice to that effect is respectfully

solicited.

Please charge any fees due in connection with this response to Deposit Account No. 50-1387.

Respectfully submitted,

Date: _November 9, 2006_

__/Scott C Harris/_____
Scott C. Harris
Reg. No. 32,030

Customer No. 23844
Scott C. Harris, Esq.
P.O. Box 927649
San Diego, CA 92192
Telephone: (619) 823-7778
Facsimile: (858) 678-5082